REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED		
2. Security Classification Authority:		
3. Declassification/Downgrading Schedule:		
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.		
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT		
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): COMPUTER NETWORK ATTACK: AN OPERATIONAL TOOL?		
9. Personal Authors: LIEUTENANT COMMANDER Curtis C. Lenderman, USN		
10. Type of Report: FINAL	**11. Date of Report:** 17 January 2003	
12. Page Count: 20	**12A Paper Advisor (if any):**	
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.		
14. Ten key words that relate to your paper: Information Operations, Computer Network Attack, Operational, Information Warfare, Command and Control, Levels of War, Spectrum of Conflict, Cyber Warfare, Preemptive Strike, Effects Based Targeting.		

15. Abstract:

Computer Network Attack (CNA) is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. Like other Information Operations, CNA has implications at the tactical, operational, and strategic levels of war. It can be implemented across the warfare spectrum, from peace to crisis, crisis to conflict and back to peace. The purpose of this paper is to argue that the effects of Computer Network Attack are best realized at the operational level of war. CNA applied at this level provides many benefits over the conventional physical reduction of an enemy capability, or by the use of CNA at the tactical level to achieve these goals. Although there is a great deal about CNA that is classified, this thesis will be examined strictly at the unclassified level. The well-planned use of CNA at the operational level of war has as its objective the decisions made by the enemy's leadership, and provides advantages over the purely tactical use of CNA. These advantages are realized in the following categories: pre-conflict coercion, speed of battlefield preparation/force multiplier, humane nature, focused effort, and post-crisis recovery. The planner must be aware of some disadvantages, such as unintended consequences, world opinion, precedent, and friendly-force vulnerabilities. The advantages inherent in the operational use of CNA can be realized through awareness (training and education), good use of intelligence (and CNA awareness in the Intelligence community), robust experimentation, and a dedicated and keen eye towards monitoring and shaping the international legal environment.

16. Distribution / Availability of Abstract:	**Unclassified** X	**Same as Rpt**	**DTIC User**
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-3556		**20. Office Symbol:** C	

NAVAL WAR COLLEGE
Newport, R.I.

COMPUTER NETWORK ATTACK: AN OPERATIONAL TOOL?

by

Curtis C. Lenderman
LCDR, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

17 January 2003

Abstract of

COMPUTER NETWORK ATTACK: AN OPERATIONAL TOOL?

Computer Network Attack (CNA) is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. Like other Information Operations, CNA has implications at the tactical, operational, and strategic levels of war, and can be implemented across the warfare spectrum, from peace to crisis, crisis to conflict and back to peace.

The purpose of this paper is to argue that the effects of Computer Network Attack are best realized at the operational level of war. CNA applied at this level provides many benefits over the conventional physical reduction of an enemy capability, or by the use of CNA at the tactical level to achieve these goals. Although there is a great deal about CNA that is classified, this thesis will be examined strictly at the unclassified level.

The well-planned use of CNA at the operational level of war has as its objective the decisions made by the enemy's leadership, and provides advantages over the purely tactical use of CNA. These advantages are realized in the following categories: pre-conflict coercion, speed of battlefield preparation/force multiplier, humane nature, focused effort, and post-crisis recovery. The planner must be aware of some disadvantages, such as unintended consequences, world opinion, precedent, and friendly-force vulnerabilities. The advantages inherent in the operational use of CNA can be realized through awareness (training and education), good use of intelligence (and CNA awareness in the Intelligence community), robust experimentation, and a dedicated and keen eye towards monitoring and shaping the international legal environment.

Computer Network Attack: An Operational Tool?

INTRODUCTION

LCDR Dave "Smelly" Feet sat in the ready room of his attack squadron, sipping coffee and listening to his shipmates speculate why last night's long awaited air strike against the island nation of Gilligania had been called off. He had a pretty good idea, although he couldn't share it with his shipmates. Only one year earlier he had been assigned to this area's Combatant Commander staff, and was a key player in the deliberate planning process for the Gilligania CONPLAN. As a regular representative in the Information Operations (IO) planning cell, he knew that one of the final measures available to the JTF Commander of an operation against Gilligania, after all other diplomatic efforts and flexible deterrent options had failed, was a Computer Network Attack (CNA) directed against the Gilligania Integrated Air Defense System (IADS) network. As an operational level concept, the Computer Network Attack, developed and implemented in cooperation with several agencies, including SOF, was to demonstrate to the Gilligania leadership the vulnerability of their loudly self-proclaimed infallible air defense system. Coordinating the CNA with small-scale, unmanned and precisely targeted incursions to the Gilligania air space, the adversary's leadership would be forced to recognize their inability to protect their air space with their failing IADS. This, coupled with other IO initiatives, would convince the Gilligania leadership to seek a peaceful solution to the aging regional tensions. Smelly could only guess that this plan was implemented in some form and the adversary was feeling very vulnerable and seeking the protection of diplomacy. The fact that a CNA was possible on the enemy

IADS was not completely unknown to the attack squadron leadership though, as there were also tactical applications. Indeed, pre-strike planning relied heavily on the timing and specific (geographic) effects of follow-on CNA's in the event that a manned strike was required.

Although fiction, the above "sea story" is not at all far-fetched. The story provides a very plausible example of how Computer Network Attack could be used at the operational level. The purpose of this paper is to argue that *the effects of Computer Network Attack are best realized at the operational level of war. CNA applied at this level provides many benefits over the conventional physical reduction of an enemy capability, or by the use of CNA at the tactical level to achieve these goals.* Although there is a great deal about CNA that is classified, this thesis will be examined strictly at the unclassified level.

WHAT IS CNA?

Computer Network Attack (CNA) is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.[1] Although this is not a paper about all forms of Information Operations (IO), it is important to gain a basic understanding as to where CNA fits into the IO toolbox. As shown in Figure 1, CNA is but one IO capability available to the commander. A good IO plan may incorporate any number of these capabilities and related activities to produce effects in an integrated fashion. For IO to work properly, operators must understand the environment, assess their interests and the

[1] Joint Chiefs of Staff, Joint Doctrine for Information Operations (Joint Pub 3-13), (Washington, D.C.: Oct 9, 1998), I-9.

adversary's pressure points and then use whichever capability or related activity that will best effect the adversary. [2]

INFORMATION OPERATIONS	
Capabilities	**Related Activities**
Computer Network Attack	Public Affairs
Deception	Civil Affairs
Destruction	
Electronic Warfare	
Operations Security	

Figure 1, Information Operations Capabilities and Activities[3]

Although many facets of CNA are only discussed in classified publications (such as the classified appendix to JP 3-13), the best starting point to understanding its nature and issues is the study of the unclassified Joint Staff guidance on Information Operations. Like other Information Operations, CNA has implications at the tactical, operational and strategic levels of war, and can be implemented across the warfare spectrum, from peace to crisis, crisis to conflict and back to peace. The remainder of this paper will identify the intended effect of CNA at each of these levels, and discuss the advantages and disadvantages to the use of CNA at the operational level.

INTENDED EFFECTS OF CNA

The aim of CNA is to deny information to an adversary by disrupting and degrading his information collection capabilities, selectively disrupting his information systems, and neutralizing or destroying his information nodes and links.[4] The effect of

[2] Joint Forces Staff College, Information Operations: The Hard Reality of Soft Power, (Norfolk, VA: 2001), 13.
[3] Ibid.
[4] Department of the Army. Information Operations. (U.S. Army Field Manual 100-6), (Washington, D.C.: Aug 27, 1996), 3-6.

this information denial depends on the level of war at which CNA is executed. This information pertains not only to information for human consumption, but to the vast amount of information that is exchanged between the nodes of a highly technical and computer driven infrastructure. An effective CNA attack may go unnoticed by humans, if that is the intent, or may be constructed to be obvious to humans for the advantages and impact it entails.

A *strategic* use of CNA would most likely involve a CNA of which the impact was made public for the future deterrent benefit to our nation.[5] For example, a legitimate use of a CNA against a state that overtly sponsored terrorism would not only further the President's policy on state sponsored terrorism, but would be a clear warning to other nations of our capabilities. Thus, CNA would be yet another mailed fist in our velvet glove of diplomacy; a capability, much like nuclear weapons, that we would prefer not to use, but are capable of and willing to do so. In the strategic use of CNA, the intended effect is the decision making of the adversary's leadership. This use of CNA would most likely be used in the *peace-crisis* portion of the spectrum of war.[6]

On the other end of the spectrum of war is the *tactical* use of CNA. On this level, a CNA could be overt or covert, with the primary effect not the decision making of the adversary's leadership, but the direct consequences of the CNA to the adversary's military systems.[7] In the example provided in the beginning of this paper, the tactical use of CNA would be the degradation of the enemy IADS with the effect of making our

[5] Joint Chiefs of Staff, II-2 (Figure II-1) and II-10.
[6] Ibid.
[7] Ibid, II-2 (Figure II-1) and II-11.

strike more effective with less risk. This use of CNA occurs during the *conflict* stage of the spectrum of war. [8]

In the middle is the *operational* level use of CNA, of which the remainder of this paper will focus. The operational use of CNA has as its target the decision making of the adversary's leadership, but at a point on the spectrum of conflict closer to *crisis-conflict*[9].

The opening example provides some insight into just what the operational use of CNA might look like. Now we can define some distinct advantages to the operational use of CNA, demonstrating its potential effectiveness and increased usability at this level.

ADVANTAGES OF CNA AS AN OPERATIONAL TOOL

Pre-Conflict Coercion . As demonstrated in the opening example, CNA may provide a step between crisis and conflict outside of diplomatic channels. That is, CNA provides a sort of "soft-blow" to the enemy's head to help him decide if he is looking for a fight. At this point in a crisis, both parties have usually been influenced by much more than the original point of contention. These outside influences may stem from relationships with allies, statements made in anger, policy enacted on misinformation, or any number of variables. This "soft-blow" may be just the thing that allows an opportunity for reconsideration, as it changes the equation and allows the adversary to come up with a new solution. An additional advantage of using CNA in pre-conflict is its possible reversibility. If the effect of the CNA does not coerce the adversary's leadership to steer away from conflict, the promise of the reversal of the CNA's effect (if possible) may be adequate incentive. If nothing else, it may provide our leadership with

[8] Joint Chiefs of Staff, II-2 (Figure II-1) and II-11.
[9] Ibid, II-2 (Figure II-I) and II-10.

something “to give” in negotiations, possibly allowing the adversary to save face by demanding this concession from our leadership. Besides the advantage offered in this regard, this same CNA may provide benefits for the follow-on operation (if conflict occurs), whether they be further battlefield preparation or part of a deception operation. A well thought-out CONOP will ensure that any CNA planned as a flexible deterrent option dovetails into any possible follow-on operations conceived.

Speed of Battlefield Preparation/Force Multiplier. The observed effects of a selective CNA may provide intelligence gatherers with critical targeting information with regard to the Command and Control Infrastructure. To be more precise, intelligence gatherers could glean the *significance of different nodes and links* by interpreting the effects of a CNA, thereby drastically shortening the target list. Additionally, some of these nodes may be targeted with CNA vice traditional kinetic means, further shortening the conventional target list. Now that the kinetic target list is minimalized, CNA could be more carefully tailored to impact the defenses of these targets, either in the form of a degraded IADS, or in a more simple adversary by cutting off warning orders promulgated via an automatic switched telephone system. If the kinetic target is a mobile launcher, for example, the CNA would be directed at the means by which its movement is orchestrated. This example has worked its way from the operational level to a level that is hard to discern between operational and tactical. In the event that the adversary avoids conflict or sues for peace due to the degradation of his systems, then the CNA was an operational success. If not, then the resulting kinetic attack will be numerically more successful than otherwise, with fewer sorties (or cruise missiles), and with fewer casualties on both sides.

Another advantage of CNA with regard to battlefield preparation is a quicker reaction time by friendly forces when confronted with an escalating situation. Instead of waiting for more friendly forces to arrive in-theater, while the enemy also continues to build-up at a rapid rate, CNA may allow a building force to respond to enemy aggression before the adversary expects it or is prepared for it. CNA may also allow friendly forces to preempt the normal deployment of enemy forces by attacking their computer infrastructure supporting enemy deployment efforts, such as public transportation controls, communication nodes and links, and the public electrical distribution system.

It is in the areas of pre-conflict coercion and battlefield preparation that CNA planners have their biggest challenges with the legal aspects of this capability. Once a conflict has begun, CNA capabilities fall somewhat more easily into the norms of the law of armed conflict, although many of these norms are yet to be established in this arena.[10] Before the conflict, however, the "good guys," without proper caution and guidance, can become the "bad guys." If the world community has difficulty accepting a nation's right to conduct a preemptive kinetic strike, what then will they think of a preemptive "soft" strike on some dual-use (civilian/military) network or infrastructure? These legal questions are of significant interest to the international legal community and are receiving a great deal of attention as the world's capabilities in cyber-warfare grow.[11] Although addressing the wide ranging legal aspects of CNA is beyond the scope of this paper, for now it is enough to know that international norms have not yet been established and that

[10] Schmitt, Michael N. and Brian T. O'Donnell, Computer Network Attack and International Law. (U.S. Naval War College, Newport RI: 2002), 5-6.
[11] Schmitt and O'Donnell, 6.

the rules that govern CNA will likely differ among peacetime, crisis, and conflict situations.[12]

Focused Effort. A key benefit to the use of CNA at the operational level is the ability to focus the CNA on a particular network or node in an effort to achieve specific effects. In the current environment, where the trend is towards "effects based targeting," CNA offers an advantage over kinetic methods in the area of experimentation. The nature of CNA gives experimenters the ability to predict with some level of accuracy the likely immediate effects, as well as second and third order effects, of a focused CNA. While these effects are more predictable at the tactical level, a better understanding of these effects will aid in predicting the ultimate effect on the adversary's leadership at the operational level. Although predicting the actions of the adversary's leadership is still more art than science, CNA gives the operational commander more methods to effect the adversary's decision making than kinetic means alone.

Another element related to a focused effort is that of timing. Whereas a kinetic attack requires the precise orchestration of many moving parts to execute on schedule and with minimal losses, a CNA is much more likely to be executed at precisely the chosen time, with the added advantage of immediate termination (possibly) if desired. This positive characteristic of CNA also lends itself well to enhancing a kinetic strike if so coordinated at the tactical level.

Humane Nature. At the tactical level, CNA appeals to the humane senses of the attacker, but at the operational level the intent is to appeal to the humane senses of the

[12] Busby, Daniel, Colonel, U.S. Army. "Peacetime Use of Computer Network Attack." Unpublished Research Paper, (U.S. Army War College, Carlisle Barracks, PA: 2000), 12.

adversary's leadership. In the opening example, the CNA demonstrated to Gilligania's leadership that his IADS was incapable of protecting his population, and therefore appealed to his sense of duty to protect his people by suing for peace or continuing along diplomatic channels before a crisis resulted in conflict. Again, at the operational level, CNA is being used to effect the decision making of the adversary's leadership.

The added benefit of this characteristic of CNA is the lack of backlash likely from other nations. This may result in added world support to further actions in the current crisis, or possibly give increased credibility to our nation in future crisis or conflicts. Most importantly though, CNA may prevent unnecessary harm to civilians who are already struggling under a harsh regime.

Post-Crisis Recovery. The last advantage of CNA to be discussed is that of a speedy and cost-effective post-crisis recovery. First, we will dispense of the tactical use of CNA and post-conflict recovery. It is easy to shoot ahead to the conclusion that a conflict fought using CNA as a tactical tool would provide the benefit of a more speedy and cost-effective recovery. This would greatly benefit the victor, as the rebuilding of the country and restoration of services to the citizens would be significantly easier. But we are discussing not the tactical use of CNA but the operational use. At the operational level, we wish to impact the adversary's decision to wage war. A traditional kinetic strike may only serve to further the enemy's fervor for war. Making martyrs of dead civilians, the enemy is likely to muster more world support for his cause and may seek vengeance on his attacker. A CNA on the other hand, may not only convince the enemy that he cannot effectively wage war, but provides him with a great incentive to give up his military objective and revert back to a peaceful stance. That incentive is the rapid

return of services to his citizens without the need for outside assistance or support. Not only does he protect his flock, but he may gain popularity at home by successfully "negotiating" the return of these services, saving face with his peers and possibly retaining his office. Again we see that if these CNA efforts fail at bringing peace, they can support further operations in conflict at the tactical level.

DISADVANTAGES OF CNA AS AN OPERATIONAL TOOL

Above we discussed several advantages that CNA offers as an operational tool. Here we will examine several reasons which may inhibit the use of CNA in the manners discussed.

Unintended Consequences. Unintended consequences of traditional kinetic strikes have often been those of collateral damage and civilian deaths. The same can be true of CNA used against an enemy if it causes unforeseen effects. At the operational level, these effects may be caused by unforeseen enemy reactions to a CNA, such as enemy leadership shutting down key infrastructure nodes in an effort to protect them from further attack. Other examples are enemy leadership retaliation in the form of human atrocities on an indigenous population, or an irrational leader's intentional damage to his own vital infrastructure such as air traffic control, resulting in civilian deaths that he attributes to his attacker in an effort to turn world opinion.

These unintended consequences at the operational level should not be confused with those stemming from a tactical miscalculation. An example of unintended consequences of a tactical CNA would be an attack having effects outside of the intended node or network due to unforeseen links or relationships in the enemy's infrastructure,

thus causing collateral damage that may cause harm to civilian or other possibly unlawful targets.

World Opinion. In this era of globalization, which many attribute to computer network capabilities and the Internet, our military use of this medium will likely be frowned upon by others, much the same as their reluctance to allow weapons in space.[13] The strongest complaints are likely to be voiced by those states that continue to profit from this technology, but who are also the most vulnerable to its military use. Although CNA may be viewed by some as "warfare on the cheap," these states may not have the significant resources required to support a robust CNA defense or a retaliatory CNA offensive capability.[14] Therefore, open acceptance of military ventures into cyber-space only puts these states at a disadvantage with no counter-balancing "up side."

Unlike the question of "weaponizing" space, which has been addressed by international talks and treaties, the notion of cyber-warfare has not yet developed to the point that international norms have been established.[15] These norms will be developed in time as nations grow to understand the impacts of such use of technology. Until this occurs, the potential CNA aggressor stands to be viewed as the "bad guy" regardless of his claim to reduced civilian casualties or desired postponement of physical hostilities.

Precedent. The publicly acknowledged use of CNA at the operational level has not yet occurred, so we can only speculate on the repercussions of such action. The first publication of the tactical use of CNA occurred during the Kosovo conflict, when the US penetrated Yugoslavia's military computers and placed false radar images on Serbian

---

[13] "The Next Battlefield May Be In Outer Space," New York Times Magazine, 5 August 2001, 2. <http://ebird.dtic.mil.> (6 August 2001).
[14] Schmitt and O'Donnell, 4.

anti-aircraft networks, with very little note taken by the public at large.[16] For the discussion of precedent, there is a vast difference between this type of tactical CNA conducted *during* hostilities, and the notion of CNA directed at an adversary in the pre-conflict stage.

If an operational CNA does not have its immediate intended effect on the adversary's leadership decision making (and possibly even if it does), the risk exists that an adversary (and the world watching) may view the use of CNA as the premature start of hostilities. This will be a precedent similar to that of the much-discussed preemptive strike. This precedent will be a strong factor in influencing the development of future accepted international norms in this arena. Therefore, by setting the wrong precedent, we may make ourselves unnecessarily vulnerable to the same treatment by militarily weaker states.

Friendly-Force Vulnerabilities. Turning this entire conversation thus far on its head brings the quick realization that our own forces and national infrastructure is vulnerable to some extent to the same CNA that this paper proposes.

> The threats facing our nation's information infrastructure come from state-sponsored cyber-warriors, terrorists, hackers, insiders, multinational corporations, foreign intelligence services, and others. Anyone with a modicum of new technology and computer skills is suddenly able to effectively target and penetrate information systems. "To make attacking more convenient, there are about 30,000 hacker-oriented sites on the Internet, bringing hacking—and terrorism—within easy reach of even the technically challenged."[17] [18]

---

[15] "The Next Battlefield May Be In Outer Space," 11.
[16] Fulgham, David A., "Yugoslavia Successfully Attacked by Computers," Aviation Weekly and Space Technology, 23 August 1999, Vol. 151, No.8; 31-32.
[17] "Bracing for Guerilla Warfare in Cyberspace," Lkd, CNN INTERACTIVE, <http://www.cnn.com/tech/specials/hackers/cyberterrror/>(8 October 1999), quoted in Busby, 3.
[18] Busby, 3.

While there are many references available that discuss the need for a vigilant defense and the methods by which this may be achieved, that is not the focus of this paper. As important as an enemy's capability to direct a CNA at the United States or U.S. forces is the enemy's *desire or willingness to pursue this path.* Again, we are not so much concerned about the enemy's capabilities as the decisions made be the enemy's leadership. Much like nuclear weapons, there is a dilemma that exists. We could choose to be the first to exploit this weapon to gain the advantage while accepting the risk of opening the door for similar use by others in retribution. A first-strike CNA on an adversary may prompt him to retaliate-in-kind whereas the absence of the offensive CNA may have provided him no desire (or legitimacy) to do so. The flip-side of that coin is to hold this capability in reserve with the desire to delay the introduction of possibly larger-scale cyber-warfare until we are better prepared to defend against it, while losing the near term advantages previously discussed.

RECOMMENDATIONS

To this point we have identified the usefulness, advantages and disadvantages of CNA at the operational level in effecting the decisions of the adversary's leadership. We will now turn to recommendations for ensuring that the capability is developed and understood by operational planners. There are four basic categories that must be addressed in order for our defense organization to fully realize the potential of CNA at the operational level: Awareness, Intelligence, Experimentation, and Legal.

Awareness. There are two key aspects of awareness that must be addressed to gain the advantages of CNA: Training and Education.

The first aspect pertains to the actual technical capabilities to develop and conduct CNA. Better termed as training than education, this aspect of awareness requires that a talent pool of qualified information warriors be developed and sustained. Both through active recruiting and through the adaptation of existing skills groups, the Department of Defense must ensure that this talent pool exists (not necessarily in DoD) and is available to provide the service required of the Combatant Commander.

The second aspect of awareness, education, is essential to ensure the Combatant Commander's planners are aware of the level of capabilities available so that they can integrate them with other IO initiatives and properly assess enemy and friendly vulnerabilities and constraints.[19] This education should occur at both the classified and unclassified level as appropriate. As indicated in the excerpt below, the lack of awareness of CNA capabilities can be a stumbling block at many levels, from acquisition of needed tools and personnel, to the actual approval for the use of this capability.

> The current perceived lack of use of CNA weapons can also be attributed to the fact that many senior officers are not familiar with them. They grew up on a military filled with kinetic solutions, and unless they are educated on the potential effects of these new weapons, their first decision is often to not use them. Likewise, if a CNA program is kept behind the green door in a compartmented cell and brought out only in a moment of crisis, its use will often not be approved. Senior leaders must be educated and read into programs that allow them to understand the capabilities of CNA. Only then can they appreciate its capabilities and be more inclined to use these weapons when the opportunity arises.[20]

This awareness can be achieved through such avenues as service school curriculums, engagement plans, and readiness reporting systems, plus general capabilities

---

[19] Joint Chiefs of Staff, V-3.

[20] Joint Forces Staff College, 66.

awareness through technical publications, newsletters, classified web-based "user-pull" products, etc.

Because CNA must be effectively integrated with other war fighting capabilities, and other forms of IO in particular, this awareness through education is essential to successful coordination among all of the various agencies involved.

Intelligence. CNA at the operational level requires a wide range of intelligence types supporting very different types of decision making by friendly force planners. Due to the effects desired by the operational use of CNA, the highest priority must be given to intelligence supporting the Combatant Commanders' decision regarding the CNA's likely impact on the adversary leader's decisions. Before this can happen though, the Combatant Commander must be provided some basic options, which can only be generated by matching specific enemy vulnerabilities with the friendly capabilities available (or useable). This requires early and ongoing intelligence needs. Finally, there is the very technical and possibly real-time intelligence needs in support of the CNA practitioner.

In order for these varied requirements to be met by the intelligence community, they must be aware of friendly force CNA capabilities, so that in conjunction with early and well prepared requests for intelligence, they can anticipate needs and recognize intelligence opportunities which match their available skill sets.

Experimentation. A key element of the capabilities development and the required awareness previously discussed is the inclusion of CNA in exercises and war fighting experiments.[21] The technical and tangible nature of *tactical* CNA lends itself

[21] Joint Chiefs of Staff, VI-2.

well to experimentation, but unfortunately the operational application of CNA is much more art than science, due to the uncertain nature of predicting the enemy's response to these actions. Certainly, experimentation will provide vast data to support the improvement of friendly CNA defense, thus making CNA a more usable tool, and possibly removing some risk from an inaccurate assessment of an enemy's reaction when CNA is applied at the operational level.

Legalities. "...while by definition CNA is a current war fighting capability of the United States, some would say that it is so limited by legal, political, and security constraints as to make it virtually useless to the combatant commanders."[22]

As the above quote attests, possibly the biggest stumbling block to the use of CNA at any level of war are the legal concerns associated with any new capability that can be deemed "unconventional." Fortunately CNA is not the first capability that could be deemed "unconventional." There were other "unconventional" capabilities that came before it, such as airplanes, land mines, chemical weapons, and nuclear weapons. A vigilant and dedicated effort can ensure that the international community doesn't prevent us from developing the capabilities that we deem necessary for our defense, while we manipulate that same community to protect us from those things that we deem too harmful or inhumane.

Again, the required awareness previously discussed is essential in allowing all agencies involved to remain abreast of and play a part in shaping the worldwide legal

[22] Joint Forces Staff College, 64.

proceedings that will effect our ability to both realize the advantages offered by CNA at all levels of war, as well as ensuring the preparedness of our defense against this capability.

CONCLUSION

The well-planned use of CNA at the operational level of war has as its objective the decisions made by the enemy's leadership, and provides advantages over the purely tactical use of CNA. These advantages are realized in the following categories: **pre-conflict coercion**, **speed of battlefield preparation/force multiplier**, **humane nature**, **focused-effort**, **and post-crisis recovery**. The planner must also be aware of some disadvantages, such as **unintended consequences**, **world opinion**, **precedent**, and **friendly-force vulnerabilities**.

Military and civilian leaders concerned with the defense of the nation can best ensure the realization of the advantages inherent in the operational use of CNA through awareness (through training and education), good use of intelligence (and CNA awareness in the Intelligence community), robust experimentation and a dedicated and keen eye towards monitoring and shaping the international legal environment.

Bibliography

Busby, Daniel, Colonel, U.S. Army. "Peacetime Use of Computer Network Attack.." Unpublished Research Paper, U.S. Army War College, Carlisle Barracks, PA: 2000.

"Bracing for Guerilla Warfare in Cyberspace." Lkd. CNN INTERACTIVE. http://www.cnn.com/tech/specials/hackers/cyberterrror/>(8 October 1999), quoted in Busby.

Department of the Army. Information Operations. (U.S. Army Field Manual 100-6). Washington, D.C.: Aug 27, 1996.

Fulgham, David A. "Yugoslavia Successfully Attacked by Computers." Aviation Weekly and Space Technology. 23 August 1999. Vol. 151, No.8; 31-32.

Joint Chiefs of Staff, Joint Doctrine for Information Operations (Joint Pub 3-13). Washington, D.C.: Oct 9, 1998.

Joint Forces Staff College, Information Operations: The Hard Reality of Soft Power. Norfolk, VA: 2001.

Schmitt, Michael N. and O'Donnell, Brian T. Computer Network Attack and International Law. U.S. Naval War College, Newport RI: 2002.

"The Next Battlefield May Be In Outer Space." New York Times Magazine. 5 August 2001. <http://ebird.dtic.mil.> (6 August 2001).